Cryptographic Techniques for Blockchain

Dr. Bhaskar Mondal

Department of Computer Science and Engineering
National Institute of Technology Patna

May 2, 2022

Table of Contents

Technologies in Blockchain


Cryptography


Secure Coding

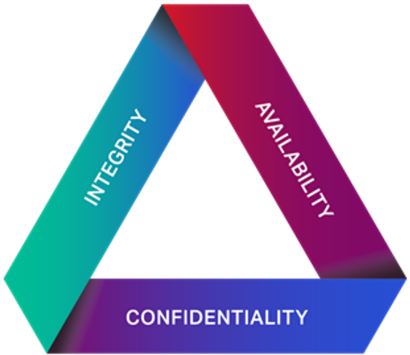

Game Theory


Database


SW Engg.


IoT

Properties of Cryptography: CIA



- Confidentiality
- Integrity
  - Data integrity
  - Non-repudiation
- Availability
- Authentication
  - Peer entity Authentication
  - Data origin Authentication
- Access Control

Blockchain

A **blockchain** is a growing list of records, called blocks, that are linked together using **cryptography**. Each block contains a cryptographic **hash** of the previous block, a timestamp, and transaction data[a].

Blockchain is a **shared, immutable ledger** that facilitates the process of recording transactions and tracking assets in a business network.[b]

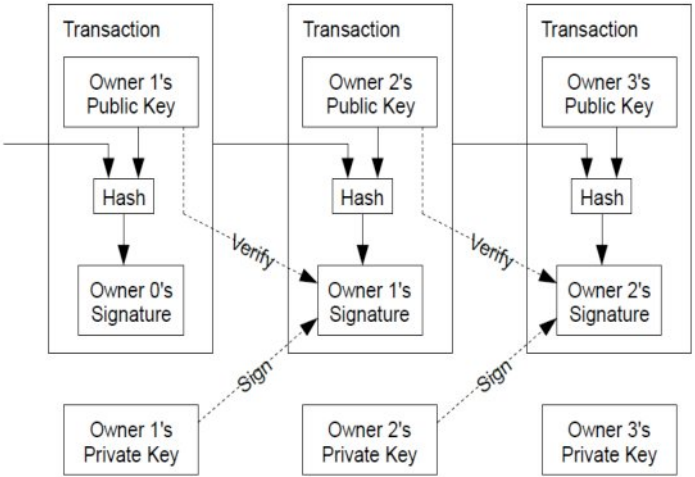
- Transparency
- Immutable data
- Decentralised
- Digital Freedom
- Anonymity & Privacy
- Security
- no intermediator
- Lower transaction fee
- Transmission efficiency

[a] https://en.wikipedia.org/wiki/Blockchain
[b] https://www.ibm.com/in-en/topics/what-is-blockchain

Crypto in Blockchain

Requirements	**Mechanism**			
	Encryption	Public key crypto-systems	Digital Signature	Hash
Peer-peer secure communication		Y		
Confidentiality	Y	Y		
Integrity: Transparency, verify a transaction				Y
Non-repudiation			Y	
Origin authentication			Y	

Crypto in Blockchain



Crypto in Blockchain

Authentication of Transaction

-Digital Signature

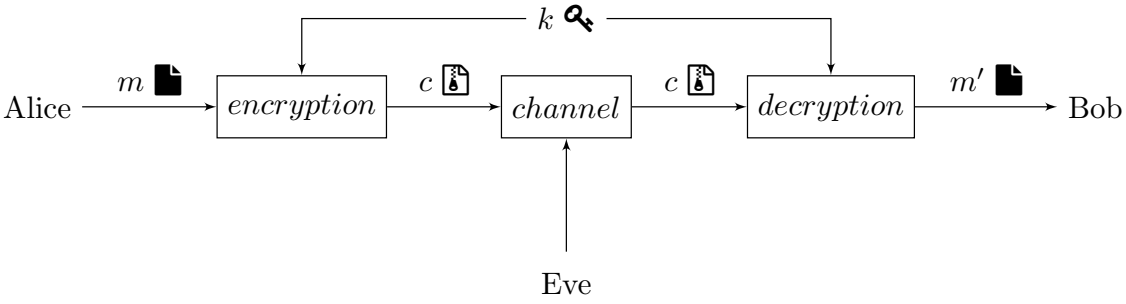
-Asymmetric key Cryptosystem

Chaining Blocks

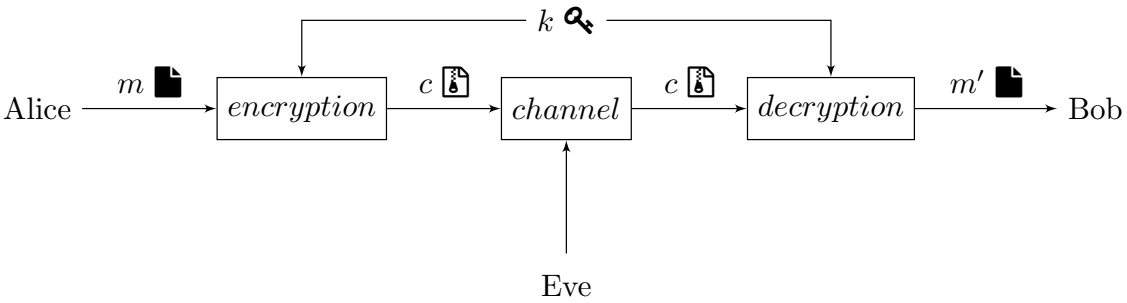
-Cryptograhic Hash

Table of Contents

Symmetric or Private Key Cryptography



Private Key Cryptography: Key Issues



If Alice and bob are at long distance and they want to talk over internet- How they share key?

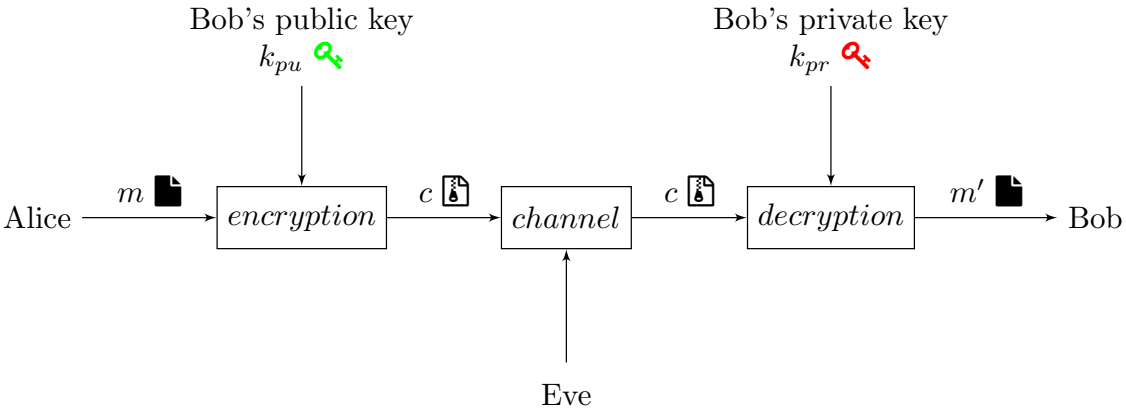
- They already met and shared the key for future use.
- Key may be send by courier (Costly - in time sense.) Not suitable in nowadays.
- Is it possible digitally using the public network?

Security

❝To keep your secret is wisdom; but to expect others to keep it is folly.❞

–Samuel Johnson

Asymmetric or Public Key Cryptography



Why Public Key Cryptosystem?

- **Key distribution** how to have secure communications in general without trusting a third-party
- **Digital signatures** how to verify a message comes intact from the claimed sender

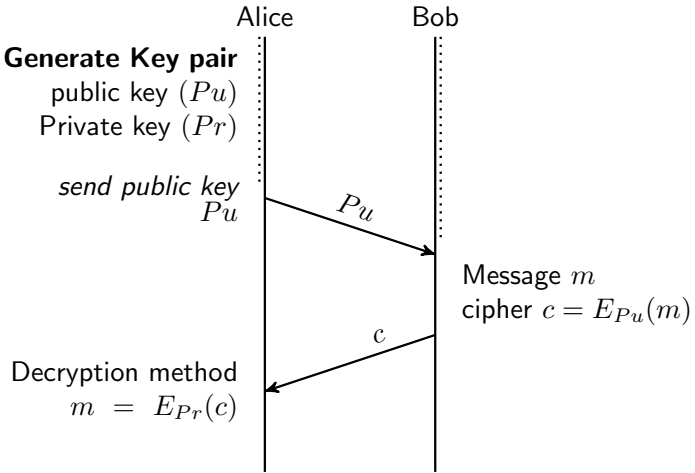
Merkle's Puzzle

"Suppose Alice and Bob wish to communicate. Bob can send a message to Alice as follows:

- first Bob creates **many puzzles**, each of a moderate amount of difficulty it must be possible for **Alice to solve** the puzzle with a moderate amount of computing effort.
  - Solution of each puzzle have an **identifier, and a session key**
- Bob sends all the puzzles to Alice, who chooses one randomly
  - Alice can communicate back to Bob which puzzle she has solved.
- Both parties now have a common key; Alice, because she solved a puzzle, and Bob, because he sent the puzzle

Any eavesdropper (Eve, say) has a harder task she does not know **which puzzle** was solved by Alice. Her best strategy is to solve all the puzzles, but since there are so many, this is more computationally expensive

Asymmetric key Cryptosystem



Public Key Cryptosystem

Public Key Cryptosystem

❝Public key like Bank Account Number and Private key is like a PIN

Uses of Asymmetric key Cryptosystem


Blockchain


Tor


Bitcoin


IoT Security


Signature


Digital certificates

Popular Asymmetric key Cryptosystem

Two of the most popular Asymmetric key Cryptosystem

RSA

-digital certificates

1977

Ron Rivest, Adi Shamir, and Leonard Adleman

ECC

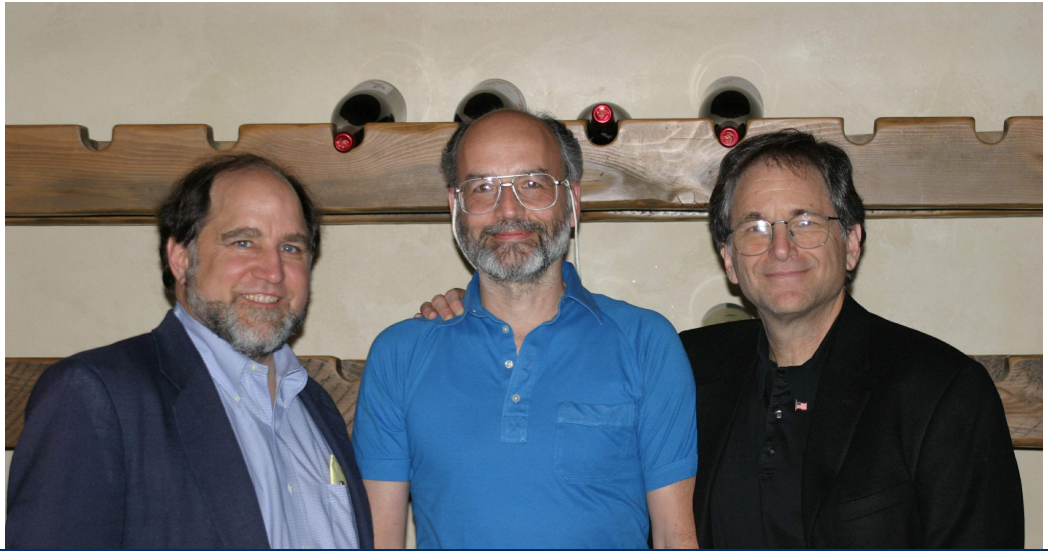
-signing data

- key exchange

1985

Neal Koblitz and Victor S. Miller

Turing Award 2002: Ron Rivest, Adi Shamir and Len Adleman



Turing Award

Turing Award

Research in cryptography has been awarded the Turing Award three times.

2015 Whitfield Diffie and Martin Hellman

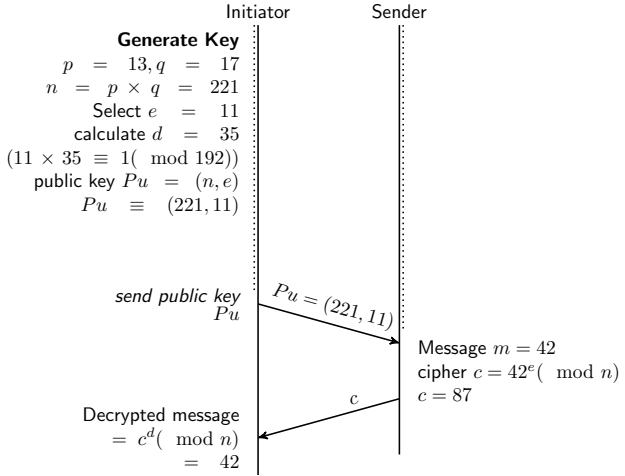
2012 Shafi Goldwasser and Silvio Micali.

2002 Ron Rivest, Adi Shamir and Leonard Adleman

RSA

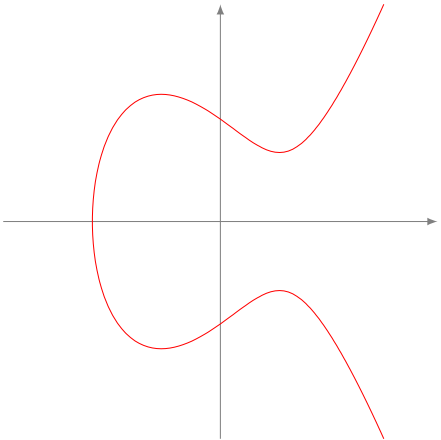
❝RSA relies on the fact that multiplying prime numbers to get a larger number is easy, while factoring huge numbers back to the original primes is much more difficult.

RSA



- p and q are two very large random prime
- $n = p \times q$ and $\phi = (p-1) \times (q-1)$
- $1 < e < \phi$ s.t. $\gcd(e, \phi) = 1$
- $1 < d < \phi$ s.t. $ed1 \mod \phi$
- Public key is (n, e)
- Private key is (d, p, q) keeping ϕ secret

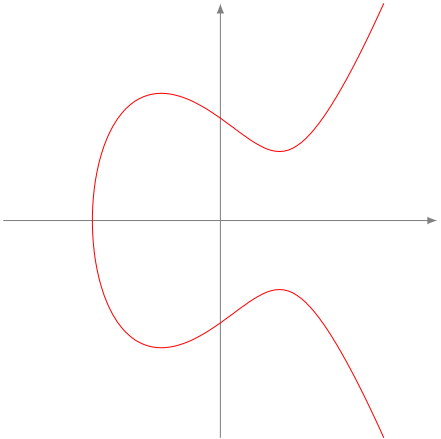
Elliptic Curve Cryptography



- Blockchain implementations like Bitcoin or Ethereum uses ECC
- ECC was invented by Heal Koblitz and Victor Miller in 1985
- Can be used for signature, encryption and decryption, and key agreement systems.
- EC have no relation with ellipses. Ellipses are generated by quadratic quation (x^2). EC are always cubic (x^3)

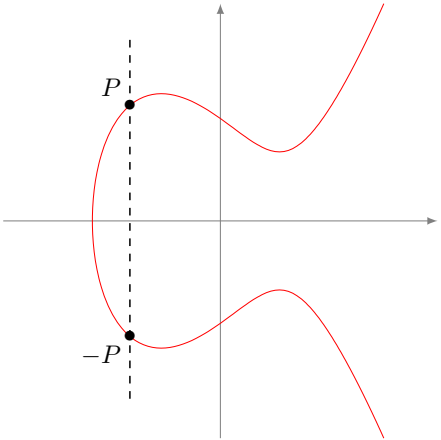
ECC: Neal Koblitz and Victor S. Miller

ECC



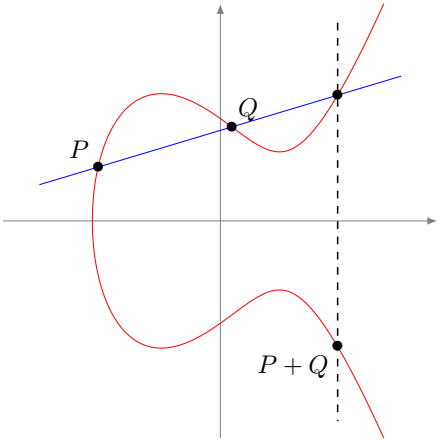
- Given by $y^2 = x^3 + ax + b$
- The Example $y^2 = x^3 + 2x + 3$

ECC



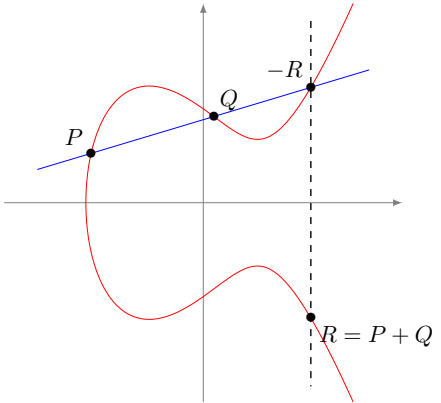
Any point on the curve can be mirrored over the x-axis and the curve will stay the same.

ECC



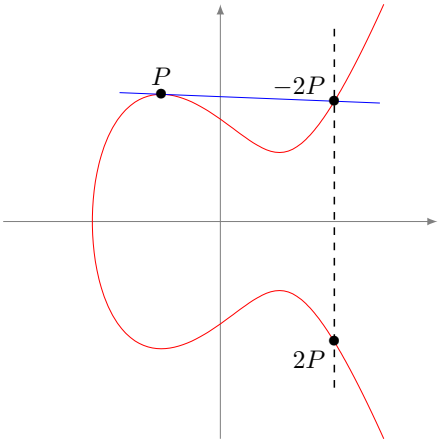
Any non-vertical line will intersect the curve in three places or fewer.

ECC: Group Operation- Addition



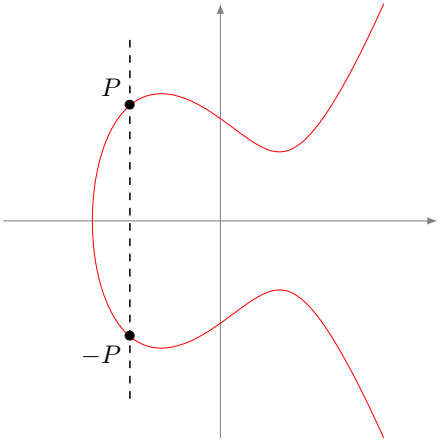
- Given two points in the set $E = \{(x, y)|y^2 = x^3 + ax + b\} \cup \{O\}$
- $P + Q = ?$
- Algebraically
  - slope $s = \frac{y_P - y_Q}{x_p - x_Q}$
  - $x_R = s^2 - (x_P + x_Q)$
  - $y_R = s(x_P - x_R) - y_P$

ECC: Group Operation- Doubling Point



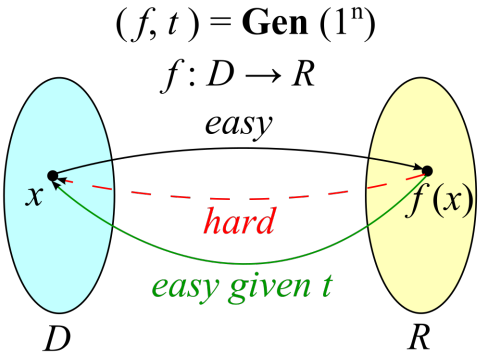
- Given a point in the set $E = \{(x, y)|y^2 = x^3 + ax + b\} \cup \{O\}$
- $P + P =?$
- $P + P = R = 2P$
- Algebraically
  - slope $s = \frac{3x_P^2 + a}{2y_P}$
  - $x_R = s^2 - 2x_P$
  - $y_R = s(x_P - x_R) - y_P$

ECC: Group Operation- Scalar Multiplication



- Given a point in the set $E = \{(x, y)|y^2 = x^3 + ax + b\} \cup \{O\}$
- Let $P \in E$ and
- $k \in Z$
- $Q = kP$
- Algebraically a Repeated Addition
  - $Q = \sum_1^k = P + P + \cdots + P$

Trapdoor function: Discrete Log Prob.

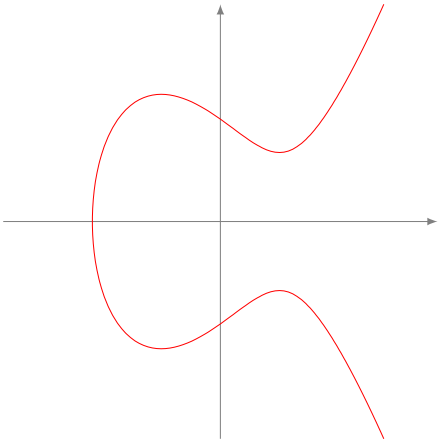


Source:
https://en.wikipedia.org/wiki/Trapdoor_function

Easy to compute in one direction, yet believed to be difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor".

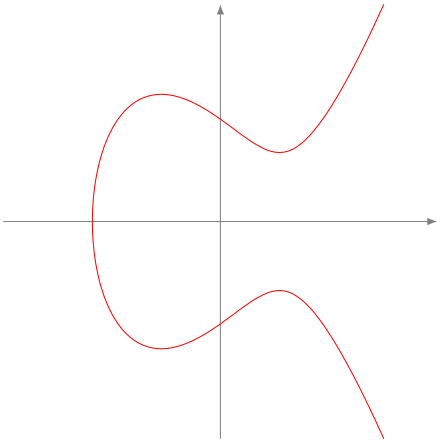
- The Scalar multiplication is considered as one way or trapdoor function
- Given $Q, P \in E(Z, pZ)$ where Q is multiple of P
- Find k such that $Q = kP$ (trapdoor)

ECC: The Base Point (Generator)



- $G \in E(Z/pZ)$ Generates a Cyclic Group on $\mod p$, where the number of point on the curve is $|E(Z/bZ)|$
- $ord(G) = n$ is the size of the subgroup
- Cofactor: $h = \frac{|E(Z/bZ)|}{n}$
  - Ideally $h = 1$

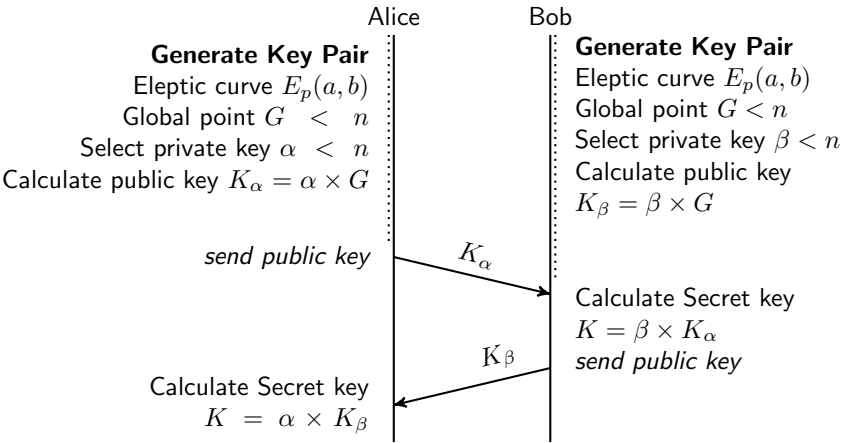
ECC: Domain Parameters



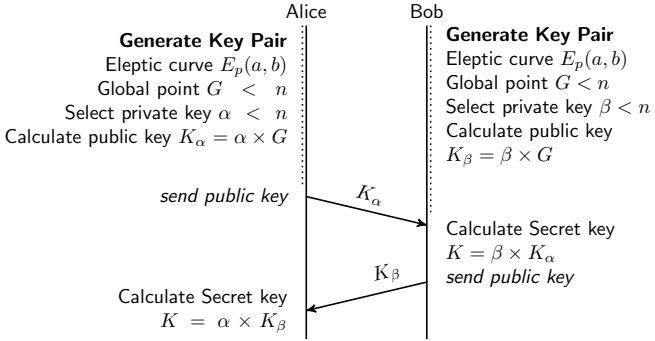
For $E = \{(x, y)|y^2 = x^3 + ax + b\} \mod p$ the domain is: $\{p, a, b, G, n, h\}$

- p is field ($\mod p$)
- a, b curve parameters
- G Generator Point
- n is $ord(G)$
- h is cofactor

ECC: Overall Process

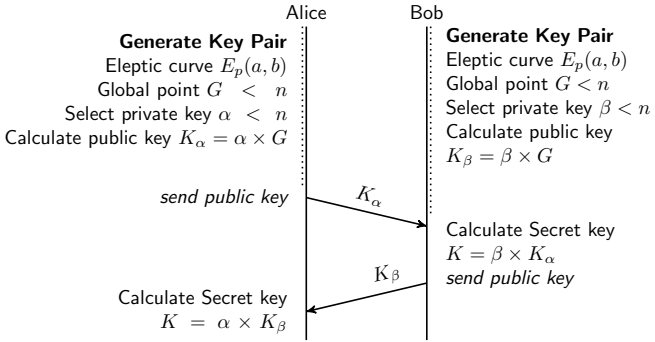


ECC: Points to note



- n is the limit on the x-axis a very large number
- private key k (α and β) is an integer and $1 < k < n - 1$
- The public keys are always points on the EC

ECC: Security



An attacker or Eavesdropper can intercept

- $E = \{y^2 = x^3 + ax + b\}$
- p is field $(\mod p)$
- a, b curve parameters
- G Generator Point
- n is $ord(G)$
- K_α public key of Alice
- K_β public key of Bob
- c_m the cipher

ECC: Example

Given

- $E : y^2 \equiv x^3 + 2x + 2 (\mod 17)$ where field $p = 17$
- Generator Point $G = (5, 1)$

Computing kG (The Cyclic Group)

- Compute $2G = G + G$ let's $k = 2$

$$s = \frac{3x_G^2 + a}{2y_G} \equiv \frac{3(5^2)+2}{2(1)} \equiv 77 \cdot 2^{-1} \equiv 9 \cdot 9 \equiv 13 (\mod 17)$$

$$x_{2G} = s^2 - 2x_G \equiv 13^2 - 2(5) \equiv 16 - 10 \equiv 6 (\mod 17)$$

$$y_{2G} = s(x_G - x_{2G}) - y_G \equiv 13(5 - 6) - 1 \equiv -13 - 1 \equiv -14 \equiv 3 (\mod 17)$$

So, **2G=(6, 3)**

ECC: Example

Given

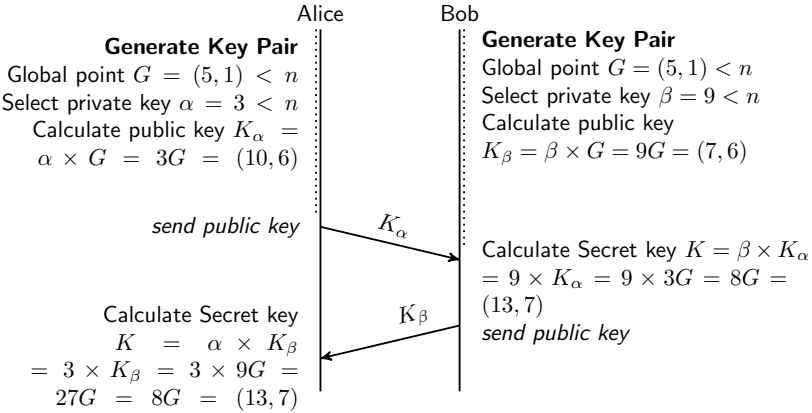
- $E : y^2 \equiv x^3 + 2x + 2 (\mod 17)$ where field $p = 17$

Computing kG (The Cyclic Group) In the same way the following can be calculated:

$G = (5, 1)$	$11G = (13, 10)$
$2G = (6, 3)$	$12G = (0, 11)$
$3G = (10, 6)$	$13G = (16, 4)$
$4G = (3, 1)$	$14G = (9, 1)$
$5G = (9, 16)$	$15G = (3, 16)$
$6G = (16, 13)$	$16G = (10, 11)$
$7G = (0, 6)$	$17G = (6, 14)$
$8G = (13, 7)$	$18G = (5, 16)$
$9G = (7, 6)$	$19G = O$
$10G = (7, 11)$	

Hence n=19, and h=1

ECC: Example



$$(27 \mod 19 = 8)$$

Owner's Private key k

- The Wallet generates a pseudo-random number R
- Takes initial affix $0x80$ of R say R'
- Apply SHA256 on R' to generate $h = H_{SHA356}(R')$
- First 4 bytes of the h are concatenated to R
- which is converted to base 28 string and considered as Private key k.

Owner's Public key P

- To produce Public key use ECC
- Public key $P = k \cdot G$

Wallet Address

- The public key is first hashed using SHA256 $h_P = H_{SHA256}(P)$
- The result h_P is again hashed using RIPEMD-160 $h_a = H_{RIPEMD-160}(h_p)$
- The binary value of h_a is the user's unique address

ECC Vulnerabilities

- side-channel attacks: differential power attacks, fault analysis, simple power attacks, and simple timing attacks, typically result in information leaks. Simple countermeasures exist for all types of side-channel attacks.
- twist-security attack or fault attack: Such attacks may include invalid-curve attacks and small-subgroup attacks, and they may result in the private key of the victim leaking out. Twist-security attacks are typically simply mitigated with careful parameter validation and curve choices.

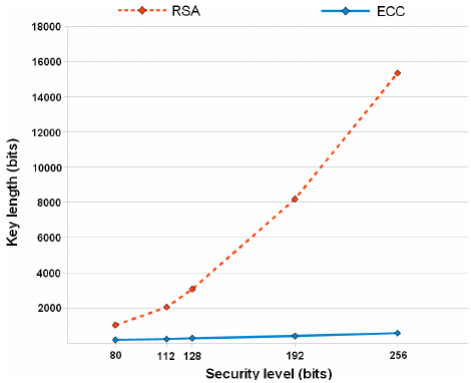
Elliptic Curve Cryptography vs RSA

Security (bits)	DSA / RSA	ECC	ECC to RSA /DSA	Valid
80	1024	160-223	1:6	Until 2010
112	2048	224-255	1:9	Until 2030
128	3072	256-383	1:12	Beyond 2031
192	7680	384-511	1:20	
256	15360	512+	1:30	

Table: Equivalence of Key strength based on effort need to break; There is no linear relationship between the sizes of ECC keys and RSA keys.

Source: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-3/archive/2012-07-10

ECC vs RSA


RSA
ECC
18000
16000
14000
12000
10000
8000
6000
4000
2000
Key length (bits)
80
112
128
192
256
Security level (bits)

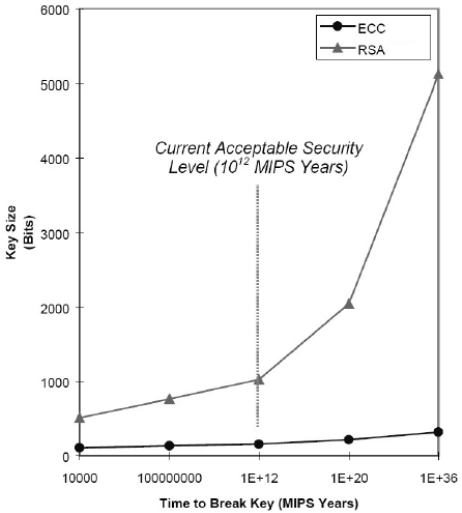

6000
5000
4000
3000
2000
1000
0
Key Size (Bits)
ECC
RSA
Current Acceptable Security Level (10^{12} MIPS Years)
10000
100000000
1E+12
1E+20
1E+36
Time to Break Key (MIPS Years)

Table of Contents

Digital Signature

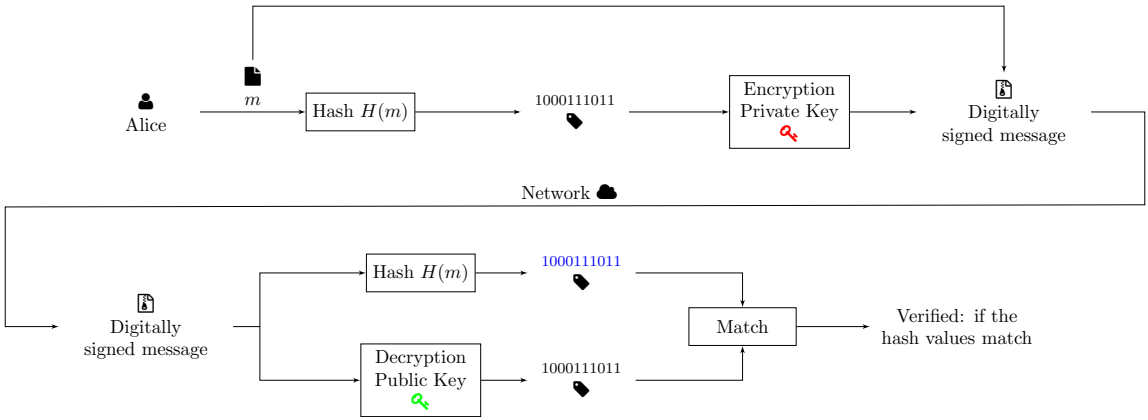
1976 Whitfield Diffie and Martin Hellman first described the idea of a digital signature scheme, but they only theorized that such schemes existed

1977 Ronald Rivest, Adi Shamir and Len Adleman invented the RSA algorithm, which could be used to produce a kind of primitive digital signature

1988 Lotus Notes 1.0, which used the RSA algorithm, became the first widely marketed software package to offer digital signatures

Turing Award 2015 Whitfield Diffie and Martin Hellman

Digital Signature



EC Digital Signature Algo. (ECDSA)

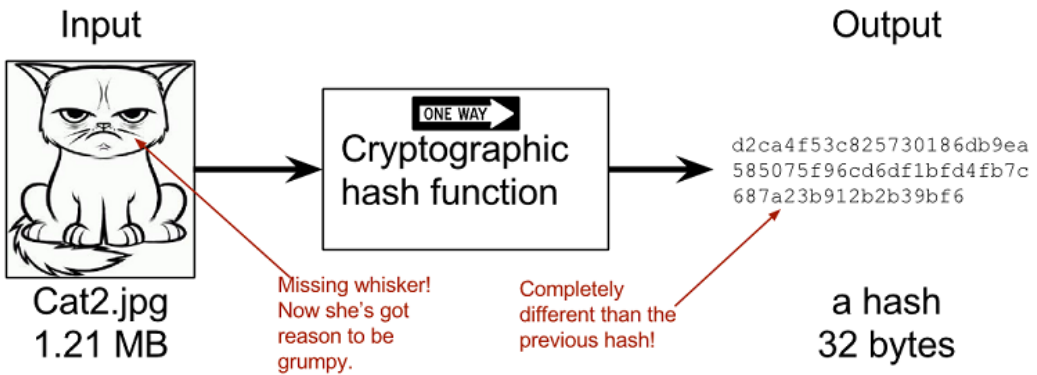
- User A generates key pair using ECC
- Then generates it's signature
  1. Select a random or pseudo-random integer $k, 1 \leq k \leq n-1$.
  2. Compute $X = k \cdot G \mod p = (x, y)$ and $r = X \mod n$ If $r = 0$ then go to step 1.
  3. Compute $k^{-1} \mod n$.
  4. Compute $e = SHA1(m)$.
  5. Compute $s = k^{-1}\{e + xr\} \mod n$ If $s = 0$ then go to step 1.
  6. A's signature for the message m is (r, s)

EC Digital Signature Algo. (ECDSA) Verification

- User A generates key pair using ECC
- Then generates it's signature
  1. A's Public Key (E, G, n, p)
  2. Verify r, and s are integer in $k, 1 \leq r, s \leq n-1$.
  3. Compute $e = SHA1(m)$.
  4. Compute $w = s^{-1} \mod n$.
  5. Compute $u_1 = ew \mod n$ and $u_2 = rw \mod n$
  6. Compute $G \cdot u_1 + p \cdot u_2 \mod p = (x_0, y_0)$ and $v = x_0 \mod n$
  7. Accept signature if$(v = r)$

Table of Contents

What is Cryptographic Hash Functions



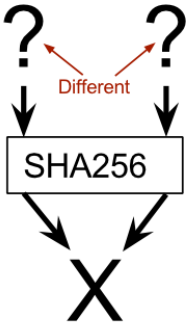
Use of Hash in Blockchain

- Generating wallet address
- Sign transaction between wallets

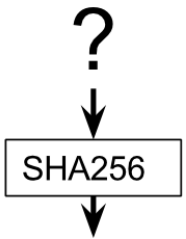
Properties of cryptographic hash functions

- $H(x)$ **easy** to compute for any given x
- Can be applied to a block of **data of any size**
- Produces a **fixed-length output**
- The hash value is **fully determined** by the data being hashed
- The hash function **uniformly distributes** the data across the entire set of possible hash values
- a small **change** to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value

Properties of cryptographic hash functions

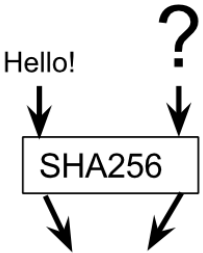


Collision resistance



334d016f755cd6dc58c53a86e1
83882f8ec14f52fb05345887c8
a5edd42c87b7

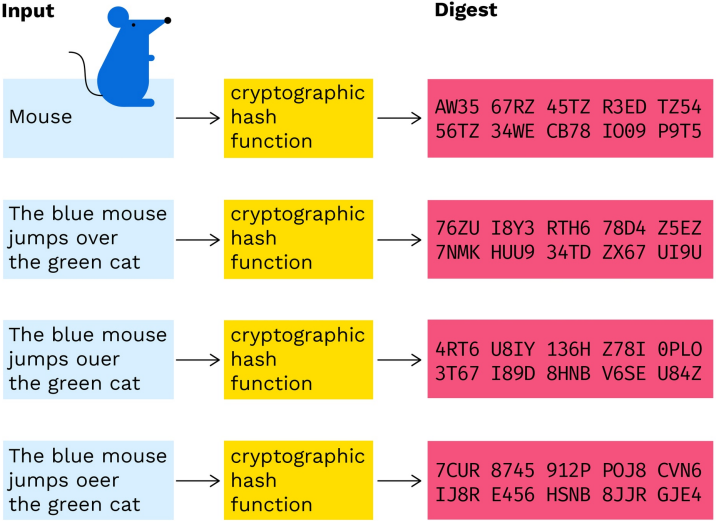
Preimage resistance



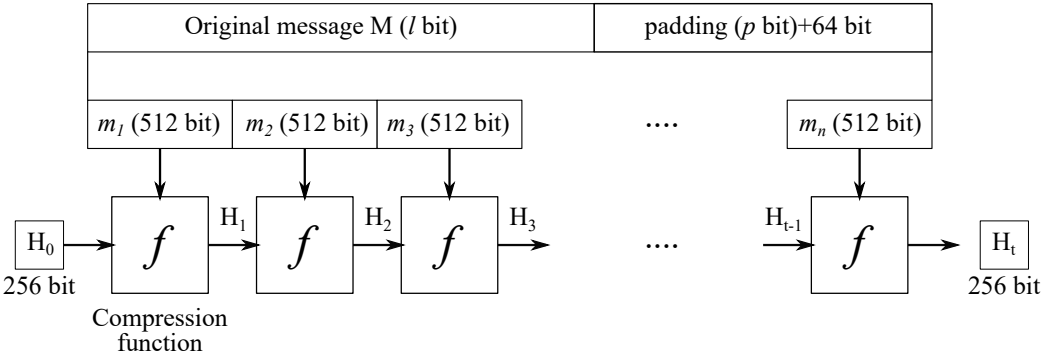
334d016f755cd6dc58c53a86e1
83882f8ec14f52fb05345887c8
a5edd42c87b7

Second-preimage resistance

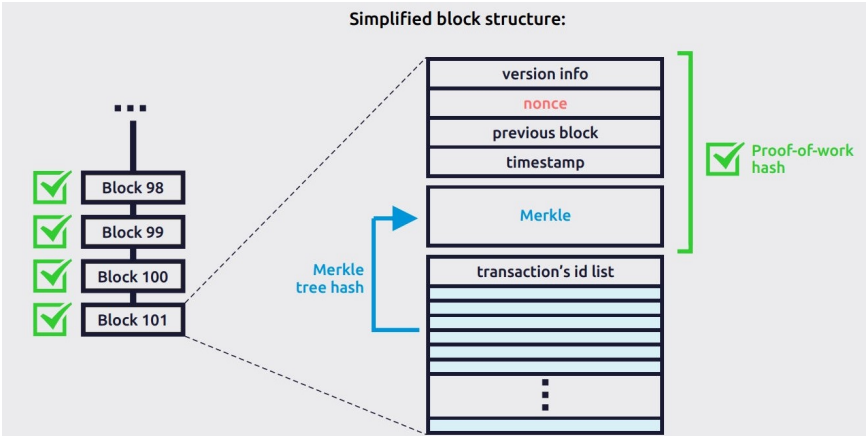
Properties of cryptographic hash fun.: Avalanche Effect



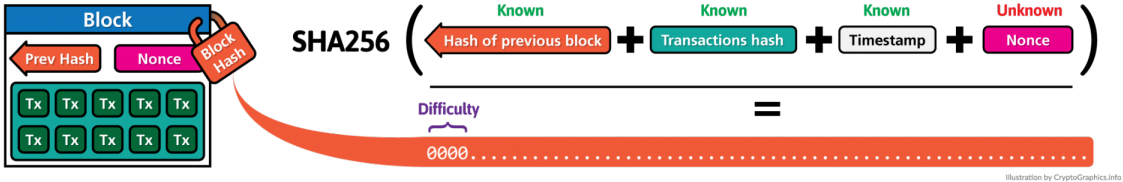
Secure Hash Algorithm 256 (SHA-256)



What does a Block Look Like?



Proof of Work



Comparing Different Hash Functions

Name	Input block size	Message limit (bits)	Hash code size (bits)	Rounds
MD5	512	$2^{64} - 1$	128	64 (4 rounds of 16)
SHA-1	512	$2^{64} - 1$	160	80 (4 rounds of 20)
SHA-256	512	$2^{64} - 1$	256	64
SHA-384	1024	$2^{128} - 1$	384	
SHA-512	1024	$2^{128} - 1$	512	
RIPEMD-160	512 bits	infinity	160 bits	160 (5 paired rounds of 16)

$2^{64} - 1$ bits $= 2,091,752$ terabytes

References I

- Stallings, W.(2006).Cryptography and network security.United Kingdom, Pearson/ Prentice Hall.
- Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). Communications of the ACM. 21 (2): 120–126. CiteSeerX 10.1.1.607.2677.
- "Secure Hashing". NIST. Archived from the original on 2011-06-25. Retrieved 2010-11-25.
- Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques (pp. 417-426). Springer, Berlin, Heidelberg.
- W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976, doi: 10.1109/TIT.1976.1055638.

Thank You